	Application No.	Applicant(s)
Notice of Allowability	09/724,337	PRICE, III, WILLIAM F.
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/15/2005*.

2. ☒ The allowed claim(s) is/are *1-4,6-13,15-22 and 24-27*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some* c)☐ None of the:
        1. ☐ Certified copies of the priority documents have been received.
        2. ☐ Certified copies of the priority documents have been received in Application No. _____.
        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
    * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    (a)☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
        1)☐ hereto or 2)☐ to Paper No./Mail Date _____.
    (b)☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of
        Paper No./Mail Date 05092005.
    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner's Statement

1.   The Drawings filed 11/27/2000, need to be submitted to the Draftsperson to be approved

for Formal Drawings.

Reasons For Allowance

2.   Status of Claims: Claims 1-4, 6-13, 15-22, and 24-27, were previously rejected, office

action dated 2/15/05, and 5, 14, and 23 were indicated as objected to claims. Claims 5, 14, and

23 have been incorporated into Independent claims, 1, 10, and 19 and thus are now allowable the

reasons the claims above are allowable are listed below:

3.   In the prior art of by generation of certificate, the prior art fails to disclose or suggest,

"prior to sending the second message, determining if the database already contains a prior client

public key associated with the client email address, if the database already contains the prior

client public key, including the prior client public key in the request for identity confirmation

sent to the client in the second message, so that the client can indicate that the server should

replace the prior client public key with the client public key"; an example of prior art that fails to

disclose the limitations above is Dyksterhouse. Dyksterhouse discloses a database that

associates key with email addresses. Clients of Dyksterhouse can access keys on the server

using a search. In the prior art of generation of a certificate and more specifically Dyksterhouse

does not disclose or suggest, the limitations above, the client does not request the server to

replace the prior client public key with the client public key, the server or certificate authority

(CA) has a certificate stored in the database that has a validity period associated with it, and

when the validity period is about to expire or has expired, the old certificate is replaced with a

new certificate, the client does not request this to happen in the prior art of generation of

certificate.

4.   In the prior art of revocation or expiration, prior art fails to disclose or suggest, "prior to

sending the second message, determining if the database already contains a prior client public

key associated with the client email address, if the database already contains the prior client

public key, including the prior client public key in the request for identity confirmation sent to

the client in the second message, so that the client can indicate that the server should replace the

prior client public key with the client public key"; an example of prior art in revocation or

expiration is, Aucsmith. Aucsmith discloses the client of Aucsmith discloses that the client

determines whether the key is in an invalidity database(revocation). Upon receipt of a key the

client performs a lookup in the invalidity database. In the prior art of revocation or expiration, a

new revocation lists is updated and given to the client or the client can download the new

revocation list. In the prior art of revocation or expiration, there is not disclosed or suggested,

"prior to sending the second message, determining if the database already contains a prior client

public key associated with the client email address, if the database already contains the prior

client public key, including the prior client public key in the request for identity confirmation

sent to the client in the second message, so that the client can indicate that the server should

replace the prior client public key with the client public key".

5.   In the prior art of key management, prior art fails to disclose or suggest, "prior to sending

the second message, determining if the database already contains a prior client public key

associated with the client email address, if the database already contains the prior client public

key, including the prior client public key in the request for identity confirmation sent to the client

in the second message, so that the client can indicate that the server should replace the prior

client public key with the client public key"; an example of prior art in key management that

does not disclose or suggest the limitations above is Van Oorshot. Van Oorschot discloses that

the trusted public keys may be updated when a policy change occurs. The policy change, which

is initiated by the system administrator or a certificate authority administrator, adds or deletes

trusted certificate authorities from a client's list. Further, Van Oorshot discloses that the system

administrator, via the policy authority would instruct the local certification authorities to update

the sets of trusted certification authority public keys of their clients. Van Oorshot discloses the

update, which contains a set of certification authority signature public key certificates would

include the public keys of each of the certification authorities. This is in contrast to the claim

limitations which claims, "prior to sending the second message, determining if the database

already contains a prior client public key associated with the client email address, if the database

already contains the prior client public key, including the prior client public key in the request

for identity confirmation sent to the client in the second message, so that the client can indicate

that the server should replace the prior client public key with the client public key". The

certificate authority in the prior art of key management is responsible for updating the keys, not

the client.

6.   In the prior art of public key method, prior art fails to disclose or suggest, "prior to

sending the second message, determining if the database already contains a prior client public

key associated with the client email address, if the database already contains the prior client

public key, including the prior client public key in the request for identity confirmation sent to

the client in the second message, so that the client can indicate that the server should replace the

prior client public key with the client public key", an example of prior art that fails to disclose or suggest the limitations above is Liu et al. Liu et al. discloses a key list is a repository for public keys. The public keys of Liu et al. are indexed by the e-mail address. The key server looks-up the status of the sender's public key and returns the status information to the recipient's viewer. The viewer displays the decrypted message and time stamp along with the sender's public key status. There is no suggestion or disclosure in the prior art of public key method, that discloses or suggests, "prior to sending the second message, determining if the database already contains a prior client public key associated with the client email address, if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key".

7.   In non-patent literature, fails to teach or suggest, "prior to sending the second message, determining if the database already contains a prior client public key associated with the client email address, if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key". An example of non-patent literature, that fails to teach or suggest, prior to sending the second message, determining if the database already contains a prior client public key associated with the client email address, if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key", is Eastlake et al. Eastlake et al. discloses

DNSSEC zone keys can be rolled over, the old public key should be left in the zone, along with the addition of the new public key. This is in contrast, to claim limitations that calls for, prior to sending the second message, determining if the database already contains a prior client public key associated with the client email address, if the database already contains the prior client public key, including the prior client public key in the request for identity confirmation sent to the client in the second message, so that the client can indicate that the server should replace the prior client public key with the client public key".

Conclusion

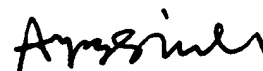Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

May 11, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100